RODO w zamówieniach publicznych – zasady przetwarzania danych osobowych

EduStrefa

Roczna opieka prawna i merytoryczna

Autor publikacji- Iwona Holka

Wskazanie wprost w Rozporządzeniu podstawowych zasad ochrony danych osobowych stanowi podstawę nowych standardów ochrony danych, obrazuje kierunek rozwoju ochrony prywatności oraz tworzy ramy dla pozostałych, szczegółowych przepisów Rozporządzenia.

1. Zasada zgodności z prawem

Rozporządzenie zawiera zamknięty katalog warunków, w jakich przetwarzanie danych może zostać uznane za zgodne z prawem. Oznacza to, że każdy proces przetwarzania danych musi opierać się na co najmniej jednej podstawie prawnej, wskazanej w Rozporządzeniu:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Nowe zasady dotyczące zgód na przetwarzanie danych osobowych

Rozporządzenie doprecyzowuje, jakie warunki powinna spełniać zgoda:

- Musi to być dobrowolne, konkretne, świadome i jednoznaczne okazanie woli. Ponadto, zgoda musi mieć charakter wyraźnego działania – oświadczenia lub potwierdzenia. W praktyce oznacza to, że formularze zgody powinny być sformułowane jasnym i czytelnym jeżykiem, tj. w sposób zrozumiały dla osoby, której dane chcemy przetwarzać. Zawiłe, nieprecyzyjne i zbyt skomplikowane formularze mogą okazać się wadliwe, a zgoda - uznana za wyrażoną w sposób nieskuteczny.
- Aby zgoda została uznana za dobrowolną - od jej wyrażenia **nie będzie można uzależniać wykonania umowy**, w sytuacji, jeśli przetwarzanie danych nie będzie niezbędne dla wykonania takiej umowy.
- W niektórych przypadkach, zgoda nie będzie uważana za dobrowolną, jeśli nie będzie możliwości wyrażenia jej osobno na rożne operacje przetwarzania danych.
- Wyrażenie zgody nie będzie uznane za dobrowolne również wtedy, gdy osoba, której dane dotyczą, **nie będzie miała rzeczywistego lub wolnego wyboru oraz nie będzie mogła odmówić ani wycofać zgody bez niekorzystnych konsekwencji**.
- Administratorzy danych będą musieli ponadto **pozyskiwać i ewidencjonować** zgody w taki sposób, aby np. w przypadku skargi osoby fizycznej, byli w stanie wykazać, że dana osoba rzeczywiście wyraziła zgodę na przetwarzanie swoich danych osobowych. Rozporządzenie nakłada na przedsiębiorców obowiązek zachowania należytego poziomu staranności. W przypadku, gdy administrator nie będzie w stanie wykazać, że pozyskał zgodę na przetwarzanie danych zgodnie z prawem, naraża się na karę administracyjną, a w niektórych przypadkach również na odpowiedzialność odszkodowawczą wobec osoby, której dane przetwarza.
- Ponadto, osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać udzieloną zgodę. W takim przypadku, jeśli administrator danych nie ma innej podstawy przetwarzania (którą może być np. niezbędność dla wykonania umowy, szczególna podstawa prawna), należy zaprzestać przetwarzania danych. Wycofanie zgody nie wpływa jednocześnie na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. O możliwości wycofania zgody należy poinformować jeszcze przed jej wyrażeniem (np. jako część klauzuli zgody).
- Wycofanie zgody musi być równie łatwe jak jej wyrażenie, np. jeśli zgoda odbierana jest telefonicznie, najlepiej umożliwić taką samą formę jej odwołania.

- Rozporządzenie w sposób szczególny chroni dzieci. W przypadku tzw. usług społeczeństwa informacyjnego (usług świadczonych na odległość drogą elektroniczną), aby przetwarzać dane osobowe dziecka poniżej 16 roku życia, konieczne będzie uzyskanie zgody rodzica lub opiekuna. Państwa członkowskie będą mogły przewidzieć niższą granicę wieku, jednak nie mniej niż 13 lat. Administrator danych będzie musiał również podjąć odpowiednie starania, aby zweryfikować, czy upoważniona osoba wyraziła zgodę na przetwarzanie danych dziecka.

- Administrator danych musi zapewnić, że zgromadzone dane osobowe są **poprawne i aktualne**, a ich **przetwarzanie przebiega bez zakłóceń**. Realizacja obu zasad nakłada na administratora szereg obowiązków polegających m.in. na wdrożeniu środków technicznych i organizacyjnych, umożliwiających korektę danych, zmniejszenie ryzyka błędów oraz usunięcie nieprawidłowych danych. Wspomniane zasady nieodłącznie powiązane są z prawem osoby, której dane są przetwarzane do żądania sprostowania i uzupełnienia danych.

- Zasada ograniczenia celu oznacza, że dane osobowe mogą być zbierane jedynie **w konkretnym, wyraźnym i prawnie uzasadnionym celu, którego osiągnięcie nie jest możliwe przy użyciu innych sposobów. Cel przetwarzania danych musi być określony w momencie ich pozyskiwania.**

- Jeśli podstawą przetwarzania danych jest zgoda, to odnosi się ona jedynie do konkretnie wskazanego celu przetwarzania. Nowy cel przetwarzania danych wymaga pozyskania nowej zgody. Dodatkowo, to na administratorze danych ciąży obowiązek informowania osób, których dane są przetwarzane o celach przetwarzania.

- Na gruncie Rozporządzenia również zakres pozyskiwanych danych musi być adekwatny i ograniczony do minimum niezbędnego dla realizacji wskazanego celu.

- Minimalizacja może polegać na wyselekcjonowaniu jedynie tych danych, które są potrzebne do danej działalności oraz na ograniczeniu okresu przechowywania danych.
  W praktyce realizacja zasady wymaga, aby przed rozpoczęciem procesu pozyskiwania, a następnie przetwarzania danych precyzyjnie określić cele i odpowiadające im rodzaje danych oraz ustalić termin usuwania i okresowego przeglądu danych.

Zasada integralności i poufności

- Zasada integralności i poufności nakłada na administratora danych obowiązek przetwarzania danych w sposób gwarantujący odpowiedni poziom bezpieczeństwa.
- Zasada integralności odnosi się do obowiązku zapewnienia, że dane nie zostały zmodyfikowane, usunięte, dodane czy zniszczone w sposób nieautoryzowany.
- Zgodnie z zasadą poufności należy zapobiegać sytuacjom, w których dane osobowe są udostępniane lub ujawniane nieautoryzowanym podmiotom czy procesom.

Zasada rozliczalności

Administrator ma nie tylko obowiązek stosować się do wymogów Rozporządzenia, w tym do wyżej wymienionych zasad, m.in. wdrażając odpowiednie środki techniczne czy organizacyjne, ale również powinien być w stanie wykazać, że stosowane przez niego metody są zgodne z Rozporządzeniem oraz skuteczne.

Zasada przejrzystości

Celem Rozporządzenia jest wzrost świadomości społeczeństwa na temat ryzyk związanych z udostępnianiem i przetwarzaniem danych osobowych. Stąd Rozporządzenie wymaga, aby wszelkie informacje, kierowane do osób fizycznych, formułowane były językiem prostym i przejrzystym. Adresat ma zrozumieć przeznaczony do niego komunikat, stąd hermetyczny język lub nadmierne skomplikowanie informacji – nie będą spełniać wymogów Rozporządzenia. Rozporządzenie kładzie nacisk na to, aby zarówno zakres udzielanych informacji jak i sposób ich przekazywania były zrozumiałe dla zainteresowanych i nie odstraszały ich swoją długością.

Zasada privacy by design

Zasada privacy by design wprowadzana jest przez art. 25 ust. 1 Rozporządzenia, zgodnie z którym „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne,

takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

Zasada privacy by default

Zasadę privacy by default określa art. 25 ust. 2, zgodnie z którym administrator będzie zobowiązany wdrożyć takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania. Dotyczyć to będzie **ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.** Omawiane środki powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych